Programmable quantum channels and measurements

Giacomo Mauro D'Ariano[1] * Paolo Perinotti[1 2] †

[1] *QUIT group, Dipartimento di Fisica "A. Volta", via Bassi 6, I-27100, Pavia, Italy*
[2] *CNR-INFM, Unità di Pavia*

Abstract. We review some partial results for two strictly related problems. The first problem consists in finding the optimal joint unitary transformation on system and ancilla which is the most efficient in programming any desired channel on the system by changing the state of the ancilla. In this respect we present a solution for $\dim(\mathscr{H}) = 2$ for both system and ancilla. The second problem consists in finding the optimal universal programmable detector, namely a device that can be tuned to perform any desired measurement on a given quantum system, by changing the state of an ancilla. With a finite dimension d for the ancilla only approximate universal programmability is possible, with $d = d(\varepsilon^{-1})$ increasing function versus ε^{-1}. We show that one can achieve $d(\varepsilon^{-1})$ polynomial, and even linear in specific cases.

Keywords: Quantum information theory; channels; quantum computing; entanglement

1 Introduction

[1] A fundamental problem in quantum computing and, more generally, in quantum information processing [1] is to experimentally achieve any theoretically designed quantum channel or detector using a fixed device, through a suitable program encoded in the state of an ancillary system. While a large branch of theoretical research in quantum information addressed the design of algorithms and of circuits to solve precise problems, a parallel research line is that of designing devices that can be programmed to achieve different tasks, just like classical computers do. Moreover, designing a programmable quantum gate or detector is a problem of relevance for example in proving the equivalence of cryptographic protocols, e. g. proving the equivalence between a multi-round and a single-round quantum bit commitment [2], or when trying to eavesdrop quantum-encrypted information. What makes the problem of gate programmability non trivial is that exact universal programmability of channels is impossible, as a consequence of a no-go theorem for programmability of unitary transformations by Nielsen and Chuang [3]. A similar situation occurs for universal programmability of POVM's [4, 5]. In both cases, it is still possible to achieve programmability probabilistically [3, 6, 7], or even deterministically [8], though within some accuracy. In establishing the theoretical limits to state-programmability of channels or POVM's the starting problem is to find the joint system-ancilla unitary or observable, respectively, which achieves the best accuracy for fixed dimension of the ancilla: this is exactly the problem that is addressed in the present paper. This problem turned out to be hard, even for low dimension. Here we will give a solution for the optimal device for programming unitary channels for dimension two for both system and ancilla. On the other hand, as regards programming observables, we will give an upper bound for the optimal ancilla dimension $d(\varepsilon^{-1})$ versus the accuracy $\varepsilon-1$ for programmable detectors. As we will see, it turns out [5] that a dimension $d(\varepsilon^{-1})$ increasing polynomially with precision ε^{-1} is possible, and even a linear dependence is achievable for specific cases. This should be compared with the preliminary indications of an exponential growth of Ref. [9]. However, even the linear dependence $d(\varepsilon^{-1})$ is still suboptimal.

*dariano@unipv.it

†perinotti@fisicavolta.unipv.it

[1] Work Presented at Workshop on Quantum Information Theory and Quantum Statistical Inference, 17-18 November 2005, Tokyo, ERATO Quantum Computation and Information Project

2 Statement of the problems

Programmable unitaries We want to program unitary channels by a fixed device as follows

$$\mathscr{P}_{V,\sigma}(\rho) \doteq \mathrm{Tr}_2[V(\rho\otimes\sigma)V^\dagger], \tag{1}$$

with the system in the state ρ interacting with an ancilla in the state σ via the unitary operator V of the programmable device (the state of the ancilla is the *program*). For fixed V the above map can be regarded as a linear map from the convex set of the ancilla states $\mathcal{A}$ to the convex set of channels for the system $\mathcal{C}$. We will denote by $\mathcal{P}_{V,\mathcal{A}}$ the image of the ancilla states $\mathcal{A}$ under such linear map: these are the programmable channels. According to the well known no-go theorem by Nielsen and Chuang it is impossible to program all unitary channels on the system with a single V and a finite-dimensional ancilla, namely the image convex $\mathcal{P}_{V,\mathcal{A}} \subset \mathcal{C}$ is a proper subset of the whole convex $\mathcal{U}$ of unitary channels and their convex combinations. This opens the following problem:

> **Problem:** *For given dimension of the ancilla, find the unitary operators V that are the most efficient in programming unitary channels, namely which minimize the largest distance $\varepsilon(V)$ of each channel $\mathscr{U} \in \mathcal{U}$ from the programmable set $\mathcal{P}_{V,\mathcal{A}}$:*
>
> $$\varepsilon(V) \doteq \max_{\mathscr{U}\in\mathcal{U}} \min_{\mathscr{P}\in\mathcal{P}_{V,\mathcal{A}}} \delta(\mathscr{C},\mathscr{P}) \equiv \max_{\mathscr{U}\in\mathcal{U}} \min_{\sigma\in\mathcal{A}} \delta(\mathscr{C},\mathscr{P}_{V,\sigma}). \tag{2}$$

As a definition of distance it would be most appropriate to use the CB-norm distance $\|\mathscr{C}-\mathscr{P}\|_{CB}$. However, this leads to a very hard problem. We will use instead the following distance

$$\delta(\mathscr{C},\mathscr{P}) \doteq \sqrt{1-F(\mathscr{C},\mathscr{P})}, \tag{3}$$

where $F(\mathscr{C},\mathscr{P})$ denotes the Raginsky fidelity [10], which for unitary map $\mathscr{C}\equiv\mathscr{U}=U\cdot U^\dagger$ is equivalent to the channel fidelity [1]

$$F(\mathscr{U},\mathscr{P})=\frac{1}{d^2}\sum_i|\operatorname{Tr}[C_i^\dagger U]|^2, \tag{4}$$

where $\mathscr{C}=\sum_i C_i\cdot C_i^\dagger$. Such fidelity is also related to the input-output fidelity averaged over all pure states $\overline{F}_{io}(\mathscr{U},\mathscr{P})$, by the formula $\overline{F}_{io}(\mathscr{U},\mathscr{P})=[1+dF(\mathscr{U},\mathscr{P})]/(d+1)$. Therefore, our optimal unitary V will maximize the fidelity

$$F(V)\doteq\min_{U\in\mathscr{U}(H)}F(U,V),\quad F(U,V)\doteq\max_{\sigma\in\mathcal{A}}F(\mathscr{U},\mathscr{P}_{V,\sigma}) \tag{5}$$

Programmable detectors The POVM of a measuring apparatus is a set of positive operators $P_i\geqslant 0$, $i=1,\dots n$, $n<\infty$ normalized to the identity $\sum_{i=1}^n P_i=I$, which gives the probability distribution of the outcomes for each input state ρ via the Born rule

$$p(i|\rho)\doteq\operatorname{Tr}[\rho P_i]. \tag{6}$$

Clearly, the most general programmable detector is described by an observable $\mathbf{F}\doteq\{F_i\}$ jointly measured on system and ancilla. The probability distribution of the outcomes is given by

$$p_\sigma(i|\rho)=\operatorname{Tr}[(\rho\otimes\sigma)F_i],\ \forall i,\forall\rho. \tag{7}$$

By taking the partial trace in Eq. (7) over the ancilla and using the polarization identity (Eq. (7) holds for all states) one obtains the POVM

$$P_{\sigma,i}=\operatorname{Tr}_2[(I\otimes\sigma)F_i]. \tag{8}$$

From Eq. (8) it follows that the convex set of states $\mathscr{A}$ of the ancilla is in correspondence via the map $\mathbf{P}_{\mathbf{F},\sigma}\doteq\operatorname{Tr}_2[(I\otimes\sigma)\mathbf{F}]$ with a convex subset $\mathscr{P}_{\mathbf{F},\mathscr{A}}\subseteq\mathscr{P}_n$ of the convex set $\mathscr{P}_n$ of the system POVM's with n outcomes. The symbol $\mathscr{P}_{\mathbf{F},\mathscr{A}}$ denotes the convex set of programmable POVM's that can be achieved with fixed observable $\mathbf{F}$ and varying state $\sigma\in\mathscr{A}$. The no-go theorem proved in [9, 5] states that for any fixed observable $\mathbf{F}$ the programmable set $\mathbf{P}_{\mathbf{F},\mathscr{A}}$ is strictly contained in $\mathscr{P}_n$, since even just the observables cannot be programmed with a fixed observable $\mathbf{F}$ and a finite dimensional ancilla. We now restrict attention to programmability of observables only, whence $n\equiv\dim(\mathscr{H})$, the case of nonorthogonal POVM's simply resorting to program observables on a larger Hilbert space. In the following we will denote by $\mathcal{O}_n$ the set of observables. The problem of measurement programmability can then be stated in mathematical terms as follows

> **Problem:** *For given dimension of the ancilla, find the joint observables* $\mathbf{F}$ *that are the most efficient in programming system observables, namely which minimize the largest distance* $\varepsilon(\mathbf{F})$ *of each observable* $\mathbf{P}\in\mathcal{O}_n$ *from the programmable set* $\mathbf{P}_{\mathbf{F},\sigma}$*:*

$$\varepsilon(\mathbf{F})\doteq\max_{\mathbf{P}\in\mathcal{O}_n}\min_{\mathbf{Q}\in\mathbf{P}_{\mathbf{F},\sigma}}\delta(\mathbf{P},\mathbf{Q})\equiv\max_{\mathbf{P}\in\mathcal{O}_n}\min_{\sigma\in\mathcal{A}}\delta(\mathbf{P},\mathbf{P}_{\mathbf{F},\sigma}). \tag{9}$$

We define the distance between two POVM's as the distance between their respective probabilities, maximized over all possible states, namely

$$\delta(\mathbf{P},\mathbf{Q})=\max_\rho\sum_i|\operatorname{Tr}[\rho(P_i-Q_i)]|\,. \tag{10}$$

The distance defined in Eq. (10) is hard to handle analytically, whence we bound it as follows

$$\delta(\mathbf{P},\mathbf{Q})\leqslant\sum_i\|P_i-Q_i\|\leqslant\sum_i\|P_i-Q_i\|_2\,, \tag{11}$$

where $\|A\|$ is the usual operator norm of A, and $\|A\|_2\doteq\sqrt{\operatorname{Tr}[A^\dagger A]}$ is the Frobenius norm.

3 Programming qubit unitaries

By some lengthy calculation we can obtain the Kraus operators for the map $\mathscr{P}_{V,\sigma}(\rho)$

$$\begin{aligned}\mathscr{P}_{V,\sigma}(\rho)&=\sum_{nm}C_{nm}\rho C_{nm}^\dagger,\\ C_{nm}&=\sum_k e^{i\theta_k}\Psi_k|\upsilon_n^*\rangle\langle\upsilon_m^*|\Psi_k^\dagger\sqrt{\lambda_m}\end{aligned} \tag{12}$$

where $|\upsilon_n\rangle$ denotes the eigenvector of σ corresponding to the eigenvalue λ_n and * denotes complex conjugation in the same fixed basis for which the operator Ψ_k have the same matrix elements as the matrix of coefficients of the eigenvector of V corresponding to eigenvalue $e^{i\theta_k}$. We then obtain

$$\begin{aligned}\sum_{nm}|\operatorname{Tr}[C_{nm}^\dagger U]|^2&=\sum_{kh}e^{i(\theta_k-\theta_h)}\operatorname{Tr}[\Psi_k^\dagger U^\dagger\Psi_k\sigma^\intercal\Psi_h^\dagger U\Psi_h]\\&=\operatorname{Tr}[\sigma^\intercal S(U,V)^\dagger S(U,V)]\end{aligned} \tag{13}$$

where

$$S(U,V)=\sum_k e^{-i\theta_k}\Psi_k^\dagger U\Psi_k\,. \tag{14}$$

and $^\intercal$ denotes transposition in the canonical basis. The fidelity (5) can then be rewritten as follows

$$F(U,V)=\frac{1}{d^2}\|S(U,V)\|^2\,. \tag{15}$$

The operator $S(U,V)$ in Eq. (14) can be written as follows

$$S(U,V)=\operatorname{Tr}_1[(U^\intercal\otimes I)V^*]\,. \tag{16}$$

Changing V by local unitary operators transforms $S(U,V)$ in the following fashion

$$S(U,(W_1\otimes W_2)V(W_3\otimes W_4))=W_2^*S(W_1^\dagger UW_3^\dagger,V)W_4^*, \tag{17}$$

namely the local unitaries do not change the minimum fidelity, since the unitaries on the ancilla just imply a different program state, whereas the unitaries on the system just imply that the minimum fidelity is achieved for a different unitary—say $W_1^\dagger UW_3^\dagger$ instead of U.

For system and ancilla both two-dimensional, one can parameterize all possible joint unitary operators as follows [11, 12] $(W_1\otimes W_2)\tilde{V}(W_3\otimes W_4)$, where

$$\tilde{V}=\exp[i(\alpha_1\sigma_1\otimes\sigma_1{}^\intercal+\alpha_2\sigma_2\otimes\sigma_2{}^\intercal+\alpha_3\sigma_3\otimes\sigma_3{}^\intercal)]\,. \tag{18}$$

The problem is now reduced to study only joint unitary operators of the form of Eq. (18). It can be proved that the coefficients of its eigenvectors are the matrix elements of Pauli matrices σ_j, $j = 0, 1, 2, 3$ where $\sigma_0 = I$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, $\sigma_3 = \sigma_z$. This means that we can rewrite $S(U, V)$ in Eq. (14) as follows

$$S(U,V) = \frac{1}{2}\sum_{j=0}^{3} e^{-i\theta_j}\sigma_j U \sigma_j\,, \tag{19}$$

with

$$\theta_0 = \alpha_1 + \alpha_2 + \alpha_3\,, \quad \theta_i = 2\alpha_i - \theta_0\,. \tag{20}$$

Through the derivation described in Appendix 4 we obtain that the fidelity minimized over all unitaries is given by

$$F(V) = \frac{1}{d^2}\min_j |t_j|^2. \tag{21}$$

where

$$\begin{aligned} t_0 &= \frac{1}{2}\sum_{j=0}^{3} e^{-i\theta_j}, \\ t_j &= e^{-i\theta_0} + e^{-i\theta_j} - t_0,\ 1 \le j \le 3. \end{aligned} \tag{22}$$

The optimal unitary V is now obtained by maximizing $F(V)$. We need then to consider the decomposition Eq. (18), and then to maximize the minimum among the four eigenvalues of $S(U, V)^\dagger S(U, V)$. Notice that $t_j = \sum_\mu H_{j\mu} e^{i\theta_\mu}$, where H is the Hadamard matrix

$$H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \tag{23}$$

which is unitary, and consequently $\sum_j |t_j|^2 = \sum_j |e^{i\theta_j}|^2 = 4$. This implies that $\min_j |t_j| \le 1$. We now provide a choice of phases θ_j such that $|t_j| = 1$ for all j, achieving the maximum fidelity allowed. For instance, we can take $\theta_0 = 0, \theta_1 = \pi/2, \theta_2 = \pi, \theta_3 = \pi/2$, corresponding to the eigenvalues $1, i, -1, i$ for V. Another solution is $\theta_0 = 0, \theta_1 = -\pi/2, \theta_2 = \pi, \theta_3 = -\pi/2$. Also one can set $\theta_i \to -\theta_i$. The eigenvalues of $S(U, V)^\dagger S(U, V)$ are then $1, 1, 1, 1$, while for the fidelity we have

$$F \doteq \max_{V \in \mathscr{U}(H^{\otimes 2})} F(V) = \frac{1}{d^2} = \frac{1}{4}, \tag{24}$$

and the corresponding optimal V has the form

$$V = \exp\left[\pm i\frac{\pi}{4}\left(\sigma_x \otimes \sigma_x \pm \sigma_z \otimes \sigma_z\right)\right]. \tag{25}$$

A possible circuit scheme for the optimal V is given in Fig. 1.

Such fidelity cannot be achieved by any V of the controlled-unitary form

$$V = \sum_{k=1}^{2} V_k \otimes |\psi_k\rangle\langle\psi_k|, \qquad \langle\psi_1|\psi_2\rangle = 0, \tag{26}$$

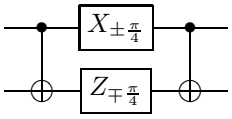

Figure 1: Quantum circuit scheme for the optimal unitary operator V in Eq. (24). W_α denotes $e^{i\frac{\alpha}{2}\sigma_W}$. For the derivation of the circuit consider that $\sigma_x \otimes \sigma_x = C(\sigma_x \otimes I)C$ and $\sigma_z \otimes \sigma_z = C(I \otimes \sigma_z)C$, where C denotes the controlled-not.

where V_1, V_2 are unitaries on $\mathscr{H} \simeq \mathbb{C}^2$. In fact, it is easy to see that in this case the fidelity is given by

$$F(U,V) = \frac{1}{4}|\operatorname{Tr}[V_h^\dagger U]|^2, \qquad h = \arg\max_k |\operatorname{Tr}[V_k^\dagger U]|, \tag{27}$$

and for any couple of unitaries $\{V_k\}$ there always exists a unitary U orthogonal to both $\{V_k\}$, whence $F(V) \doteq \min_{U \in \mathscr{U}(H)} F(U, V) = 0$.

4 Upper bound on optimal size for programmable detectors

We will now derive an upper bound for the function $d = d(\varepsilon^{-1})$, where $\epsilon = \min_{\mathbf{F}} \varepsilon(\mathbf{F})$, that gives the minimal needed dimension of the ancilla to achieve accuracy ε^{-1} in programming observables for a finite-dimensional quantum system. Clearly the function $d = d(\varepsilon^{-1})$ must be increasing, since the higher is the accuracy ε^{-1}, the larger the minimal dimension d needed for the ancilla, namely the "size" of the programmable detector.

Consider now a d-dimensional ancilla and a system-ancilla interaction U of the following *controlled-unitary* form

$$U = \sum_{k=1}^{d} W_k \otimes |\phi_k\rangle\langle\phi_k|, \tag{28}$$

where $\{\phi_k\}$ is an orthonormal complete set of vectors for the ancilla and W_k are generic unitary operators on $\mathscr{H}$. Consider then a POVM $\mathbf{E} = U\mathbf{F}U^\dagger$ of the form

$$E_i = |\psi_i\rangle\langle\psi_i| \otimes I_A\,, \tag{29}$$

where I_A denotes the identity operator on the ancilla space, and $\{\psi_k\}$ is a complete orthonormal set for the system. The observable to be approximated will then be written as follows

$$P_i = W^\dagger|\psi_i\rangle\langle\psi_i|W, \tag{30}$$

W being a unitary operator on $\mathscr{H}$, and we will scan all possible observables by varying W. For the program state of the ancilla we use one of the states ϕ_k, which give the POVM's

$$Q_i = W_k^\dagger|\psi_i\rangle\langle\psi_i|W_k\,. \tag{31}$$

This special form simplifies the calculation of the bound

in Eq. (11), which becomes

$$\begin{aligned}\delta(\mathbf{P},\mathbf{Q}) &\leqslant \sum_i \sqrt{2(1-|\langle\psi_i|W^\dagger W_k|\psi_i\rangle|^2)} \\ &\leqslant \sqrt{2}\sum_i \sqrt{2-\langle\psi_i|(W^\dagger W_k - W_k^\dagger W)|\psi_i\rangle},\end{aligned} \tag{32}$$

and using the Jensen's inequality for the square root function we have

$$\delta(\mathbf{P},\mathbf{Q}) \leqslant \sqrt{2n}\,\|W-W_k\|_2\ . \tag{33}$$

Now we can always take d sufficiently large such that we can choose the d operators $\{W_k\}$ in the unitary transformation U in Eq. (28) in such a way that for each given W there is always a unitary operator W_k in the set for which $\sqrt{2n}\,\|W-W_k\|_2$ is bounded by ε. This will guarantee that for the given observable $\mathbf{P}$ corresponding to W there is a program state for the ancilla such that the POVM $\mathbf{Q}$ achieved by the programmable detector is close to the desired $\mathbf{P}$ less than ε. The set of all possible unitary operators W is a compact manifold of dimension $h = n^2 - n$. We now consider a covering of the manifold with balls of radius $r = \frac{\varepsilon}{\sqrt{2n}}$ centered at the operators W_k. This guarantees that any W would be within a distance $\frac{\varepsilon}{\sqrt{2n}}$ from an operator W_k, which in turns implies that the accuracy of the programmable device is bounded by ε via Eq. (33). Using the volume $V = \frac{\pi^{\frac{h}{2}} r^h}{\Gamma(\frac{1}{2}h+1)}$ of the h-dimensional sphere of radius r, we obtain the number of balls needed for the covering (for sufficiently small ε, corresponding to the upper bound for the minimal dimension of the ancilla

$$d \leqslant \kappa(n)\left(\frac{1}{\varepsilon}\right)^{n(n-1)}\ , \tag{34}$$

where $\kappa(n)$ is a constant that depends on n. Eq. (34) gives an upper bound for the dimension d which is polynomial versus the accuracy ε^{-1}.

For qubits, the observable has only two elements, $P_0 = |\psi\rangle\langle\psi|$ and $P_1 = |\psi_\perp\rangle\langle\psi_\perp| = I - P_0$, and the distance in Eq. (10) can be evaluated analytically as follows

$$\delta(\mathbf{P},\mathbf{Q}) = \max_\rho 2|\,\mathrm{Tr}[\rho(P_0-Q_0)]|\,. \tag{35}$$

As regards now the programmability of all POVM's (i. e. including the nonorthogonal ones), just notice that one just needs to be able to program only the extremal POVM's in $\mathscr{P}_n$, since their convex combinations will corresponds to mixing the program state or to randomly choosing among different detectors. Then, since their maximum number of outcomes is n^2, the extremal POVM's have Naimark's extension to observables in dimension n^2, whence we are reduced to the case of programmability of observables in dimension n^2.

We will now give a programmable detector for qubits that achieves an accuracy that is linear in d. For the ancilla we use a generic d-dimensional quantum system, and relabel the dimension in the angular momentum fashion $d \doteq 2j+1$. The idea is now to design a programmable detector in which the unitary transformation corresponding to the observable $\{P_i\}$ in Eq. (30) is programmed by covariantly changing the program state of the ancilla. By labeling unitary transformations by a group element $g \in \mathbb{SU}(2)$, we write the observable to be programmed as $P_0 \doteq V_g|\frac{1}{2}\rangle\langle\frac{1}{2}|V_g^\dagger$ where $\{V_g\} \equiv (\frac{1}{2})$ is a unitary irreducible representation of $\mathbb{SU}(2)$ with angular momentum $\frac{1}{2}$, whereas the program state will be written as $W_g\sigma W_g^\dagger$, with $\{W_g\} \equiv (j)$ a unitary irreducible representation of $\mathbb{SU}(2)$ on the ancilla space with angular momentum j. As already noticed, without loss of generality we can always choose the state σ as pure. We will now show that a good choice for the program state is $\sigma = |j,j\rangle\langle j,j|$, $\{|j,m\rangle\}$ denoting an orthonormal basis of eigenstates of J_z in the irreducible representation with angular momentum j. The tensor representation $\{V_g \otimes W_g\} \equiv \frac{1}{2}\otimes j$ can be decomposed into the direct sum of two irreducible representations $\frac{1}{2}\otimes j = j_+ \oplus j_-$, where $j_\pm = j \pm \frac{1}{2}$. For the POVM $\mathbf{F}$ of the programmable detector we will use $F_0 = Z_+$ and $F_1 = Z_-$, $Z_\pm$ denoting the orthogonal projector on the invariant space for angular momentum $j_\pm$

$$F_0 = \sum_{m=-j_+}^{j_+} |j_+,m\rangle\,\langle j_+,m|\,. \tag{36}$$

Using the invariance $(V_g\otimes W_g)F_0(V_g^\dagger\otimes W_g^\dagger) = F_0$, we can write the programmed POVM as follows

$$\begin{aligned}Q_0 =& \,\mathrm{Tr}_A[(I\otimes W_g^\dagger|j,j\rangle\langle j,j|W_g)F_0] \\ =& V_g^\dagger\,\mathrm{Tr}_A[(I\otimes|j,j\rangle\langle j,j|)F_0]V_g \\ =& V_g\left(\left|\tfrac{1}{2},\tfrac{1}{2}\right\rangle\left\langle\tfrac{1}{2},\tfrac{1}{2}\right| + \tfrac{1}{2j+1}\left|\tfrac{1}{2},-\tfrac{1}{2}\right\rangle\left\langle\tfrac{1}{2},-\tfrac{1}{2}\right|\right)V_g^\dagger,\end{aligned} \tag{37}$$

where we used the only non vanishing Clebsch-Gordan coefficients $|\langle j_+,j_+|\frac{1}{2},\frac{1}{2}\rangle|j,j\rangle|^2 = 1$, and $|\langle j_+,j_-|\frac{1}{2},-\frac{1}{2}\rangle|j,j\rangle|^2 = \frac{1}{2j+1}$. Clearly, $Q_0 - P_0 = \frac{1}{2j+1}V_g|\frac{1}{2},-\frac{1}{2}\rangle\langle\frac{1}{2},-\frac{1}{2}|V_g^\dagger$, whence according to Eq. (35) the accuracy is given by $\delta(\mathbf{P},\mathbf{Q}) = 2/d$. The scaling of the dimension with the accuracy is then linear

$$d = 2\varepsilon^{-1}, \tag{38}$$

whereas the bound (34) would be quadratic $d \propto \varepsilon^{-2}$. Sublinear growth of d versus ε^{-1} is not excluded in general, but is not possible for the present model.

Appendix: Derivation of the minimum fidelity for the unitary V

Starting from Eq. (19) we will obtain Eq. (24). The unitary U belongs to $\mathbb{SU}(2)$, and can be written in the Bloch form

$$U = n_0 I + i\vec{n}\cdot\vec{\sigma}\,, \tag{39}$$

with $n_k \in \mathbb{R}$ and $n_0^2 + |\vec{n}|^2 = 1$. Using the identity

$$\sigma_j\sigma_l\sigma_j = \epsilon_{jl}\sigma_l, \qquad \epsilon_{j0} = \epsilon_{jj} = 1, \quad \epsilon_{jl} = -1\,, l \neq 0, j, \tag{40}$$

we can rewrite

$$S(U,V) = \tilde{n}_0 I + \tilde{\vec{n}}\cdot\vec{\sigma}, \tag{41}$$

where

$$\begin{aligned}\tilde{n}_j =& t_j n_j, \quad 0\leq j\leq 3, \quad t_0 = \frac{1}{2}\sum_{j=0}^{3} e^{-i\theta_j}, \\ t_j =& e^{-i\theta_0} + e^{-i\theta_j} - t_0,\ 1\leq j\leq 3,\ 0\leq j\leq 3,\end{aligned} \tag{42}$$

and we will use the exponential representation for the complex number $t_j = |t_j|e^{i\phi_j}$. It is now easy to evaluate the operator $S(U,V)^\dagger S(U,V)$. One has

$$\begin{aligned} &S(U,V)^\dagger S(U,V) = v_0 I + \vec{v}\cdot\vec{\sigma}, \\ &v_0 = |\tilde{n}_0|^2 + |\tilde{\vec{n}}|^2, \quad \vec{v} = i\left[2\Im(\tilde{n}_0\tilde{\vec{n}}^*) + \tilde{\vec{n}}^* \times \tilde{\vec{n}}\right]. \end{aligned} \tag{43}$$

Now, the maximum eigenvalue of $S(U,V)^\dagger S(U,V)$ is $v_0 + |\vec{v}|$, and one has

$$|\vec{v}|^2 = 2\sum_{i,j=0}^{3} |\tilde{n}_i|^2 |\tilde{n}_j|^2 \sin^2(\phi_i - \phi_j), \tag{44}$$

whence the norm of $S(U,V)$ is given by

$$\|S(U,V)\|^2 = \vec{u}\cdot\vec{t} + \sqrt{\vec{u}\cdot\vec{T}\vec{u}}, \tag{45}$$

where $\vec{u} = (n_0^2, n_1^2, n_2^2, n_3^2)$, $\vec{t} = (|t_0|^2, |t_1|^2, |t_2|^2, |t_3|^2)$, and $\vec{T}_{ij} = |t_i|^2|t_j|^2 \sin^2(\phi_i - \phi_j)$. Notice that the unitary U which is programmed with minimum fidelity in general will not not be unique, since the expression for the fidelity depends on $\{n_j^2\}$. Notice also that using the decomposition in Eq. (18) the minimum fidelity just depends on the phases $\{\theta_j\}$, and the local unitaries will appear only in the definitions of the optimal program state and of the worstly approximated unitary. One has the following bound on the expression in Eq. (45)

$$\vec{u}\cdot\vec{t} + \sqrt{\vec{u}\cdot\vec{T}\vec{u}} \geq \vec{u}\cdot\vec{t} \geq \min_j |t_j|^2, \tag{46}$$

and the bound is achieved on one of the four extremal points $u_l = \delta_{lj}$ of the domain of $\vec{u}$ which is the convex set $\{\vec{u},\ u_j \geq 0, \sum_j u_j = 1\}$ (the positive octant of the unit four dimensional ball S_+^4). This proves the content of Eq. (24).

This work has been co-founded by the EC under the program ATESIT (Contract No. IST-2000-29681) and the MIUR cofinanziamento 2003 and FIRB 2004-2006. P.P. acknowledges support from the INFM under project PRA-2002-CLON. G.M.D. acknowledges partial support by the MURI program administered by the U.S. Army Research Office under Grant No. DAAD19-00-1-0177.

References

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University press, 2000.

[2] G. M. D'Ariano, D. Kretschmann, D. Schlingeman, R. F. Werner, unpublished.

[3] M. A. Nielsen and I. L. Chuang. Programmable Quantum Gate Arrays. *Phys. Rev. Lett.*, 79:321–324, 1997.

[4] J. Fiurásek and M. Dušek. Probabilistic quantum multimeters. *Phys. Rev. A*, 69:032302, 2004.

[5] G. M. D'Ariano, P. Perinotti, and P. Lo Presti. Classical randomness in quantum measurements. *J. Phys. A: Math. Gen.*, 38:5979–5991, 2005

[6] M. Hillery, V. Bužek, and M. Ziman. Probabilistic implementation of universal quantum processors. *Phys. Rev. A*, 65:022301, 2002.

[7] M. Dušek and V. Bužek. Quantum-controlled measurement device for quantum-state discrimination. *Phys. Rev. A*, 66:022112, 2002.

[8] G. Vidal and J. I. Cirac. Storage of quantum dynamics on quantum states: a quasi-perfect programmable quantum gate. quant-ph/0012067, 2000.

[9] J. Fiurášek, M. Dušek, and R. Filip. Universal Measurement Apparatus Controlled by Quantum Software. *Phys. Rev. Lett.*, 89:190401, 2002.

[10] M. Raginsky. A fidelity measure for quantum channels. *Phys. Lett. A*, 290:11–18, 2001.

[11] B. Kraus and J. I. Cirac. Optimal creation of entanglement using a two-qubit gate. *Phys. Rev. A*, 63:062309, 2001.

[12] N Khaneja, R. Brockett, and S. Glaser. Time optimal control in spin systems. *Phys. Rev. A*, 63:032308, 2001.

[13] G. M. D'Ariano and P. Perinotti. On the most efficient unitary transformation for programming quantum channels. quant-ph/0509183, 2005.